

16636

REMARKS

Claims 11-20 are cancelled and Claims 21-30 are added. Claims 21-30 remain in the application. No new matter is added by the amendments to the claims.

Cancelled Claims 11-20 have been rewritten as new Claims 21-30 respectively to clarify the wording. Claim 21 amends step e. of Claim 11 to make it clear that the virtual key is generated upon detecting the at least one initiating event. Claim 29 amends the subject matter of Claim 19 to clarify that step i. is being performed.

The Rejections:

In the Final Office Action dated May 19, 2005, the Examiner rejected Claims 11, 14-16, and 18-19 35 U.S.C. 102(b) as being anticipated by McNab, et al. (US 4,937,855).

As per Claim 11, the Examiner stated:

Method of initiating a procedure within a building comprising the steps of:

- a. defining at least one initiating event for said procedure; [col.3, lines 23-31]
- b. defining at least one requirement for at least one procedure; [col.9, lines 30-60]
- c. defining at least one person to be authorized to perform said procedure; [col.8, lines 65-65]
- d. detecting said initiating event; [col.9, lines 30-50]
- e. generating a virtual key based on said requirement for said person; [col.3, lines 33-34]
- f. transmitting said virtual key to said person; [col.8, lines 43-47]
- g. detecting an entered virtual key; [col.8, lines 32-34]
- h. checking the validity of said entered virtual key; and [col. 10, lines 28-44]
- i. initiating said procedure within the building if said validity check is positive. [col.8, lines 36-40]

As per Claim 14, the Examiner stated: See col.3, lines 23-31; discusses defining different procedures for different initiating events.

As per Claim 15, the Examiner stated: See col.9, lines 30-60; discusses defining different requirements for different procedures.

As per Claim 16, the Examiner stated: See col.9, lines 30-60; discusses transmitting different virtual keys to said person for different initiating events.

000332102/00037/641328-1

16636

As per Claim 17, the Examiner stated: See col.8, lines 32-34; discusses storing said virtual key partially or completely. Applicants assume that the Examiner is referring to Claim 18.

As per Claim 19, the Examiner stated:
method according to Claim 11, further comprising at least one of the steps of:
initiating a control procedure of an elevator in said building [col.9, lines 22-25]
initiating a medical assistance procedure; [col.3, lines 25-29]
initiating a building cleaning procedure; and initiating a guest reception procedure. [col.9, lines 30-40]

The Examiner rejected Claims 12, 13, 17, and 20 under 35 U.S.C. 103(a) as being unpatentable over McNab, et al.

As per Claim 12, the Examiner stated: McNab teaches authorized persons having access to the building according to a virtual key in the form of a code or a password. McNab did not fully disclose assigning an encrypted code to said virtual key. However, it is obvious of ordinary skills in the art for the virtual key to be encrypted is an added security feature that further prevents any unauthorized persons from obtaining access any easier.

As per Claim 13, the Examiner stated: McNab teaches authorized persons having access to the building according to a virtual key in the form of a code or a password. McNab did not include adding a signature to said virtual key and identifying a recipient of said transmitted virtual key by means of said signature. However, it would have been obvious for a person of ordinary skills in the art to include a signature to the virtual key is an added authentication feature and helps unidentified persons from gaining access to the building.

As per Claim 17, the Examiner stated: McNab teaches authorized persons having access to the building according to a virtual key in the form of a code or a password. McNab did not include identifying said person with biometric characteristics. However, it would have been obvious for a person of ordinary skills in the art to include biometric characteristics is a known added authentication feature because biometric characteristics is the actual authorized person's feature that is more complex to duplicate or hack for any unidentified persons to gain access to the building.

16636

As per Claim 20, the Examiner stated: McNab teaches authorized persons having access to the building remotely according to a virtual key in the form of a code or a password but did not include transmitting said virtual key using wireless devices. However, it would have been obvious for a person of ordinary skills in the art to include wireless devices would be the conveniences of accessibility.

Applicants' Response:

The McNab et al. patent concerns a building security system for communication between building dwellers and visitors at an intercom station near the building entry (col. 2, lines 27-37). McNab et al. also discusses rapid emergency communication and building access for selected personnel based on security codes (col. 3, lines 22-28). McNab et al. does not show or suggest the transmission of the security code to dwellers, visitors or selected personnel. In col. 8, lines 32-40, McNab et al. states only that the security codes are preset and stored in a memory.

The Examiner equates the step d. of "detecting the at least one initiating event" with the entry of the security code (col. 9, lines 30-60) in the McNab et al. security system. However, Claim 21 recites in step a. that the virtual key is not even generated until the initiating event is detected. Therefore, entry of the security code in the McNab et al. security system cannot be the "initiating event of Claim 21.

Applicants' Claim 21 clarifies that step e. is performed only after step d. is performed. McNab et al. does not disclose or suggest the combination of the following steps defined by Applicants' Claim 21:

- d. detecting the at least one initiating event;
- e. generating a virtual key for the at least one person based on the at least one requirement upon detecting the at least one initiating event; and
- f. transmitting the virtual key to the at least one person.

Thus, Claims 21-30 define a method in which the virtual key is generated only when the initiating event occurs and is detected. Only then is the virtual key generated and transmitted to an authorized person. In the McNab et al. security system, the security codes are preset and stored before an initiating event occurs. See the discussion cited by the Examiner (col. 8, lines 33-34) wherein the preset security code is entered at the panel keypad.

16636

The Examiner stated that the McNab et al. security system transmits the virtual key to a person, but the discussion cited by the Examiner (col. 8, lines 43-47) describes remote programming to reset the stored codes.

Therefore, Claims 21-30 define a method whereby an authorized person can only access a building if the initiating event has indeed occurred. Examples, of such initiating events are set forth on page 3 of Applicants' specification at lines 23-25. In the McNab et al. security system, the present security codes are generated and stored before any event occurs and can be used to enter the building even if the associated event has not occurred.

The Examiner made of record but did not discuss references to Takemura et al., Wewalaarachchi et al., Coppernith et al. and Carroll et al. Applicants reviewed these references and found them to be more pertinent than the prior art relied upon by the Examiner in the rejections.

In view of the amendments to the claims and the above arguments, Applicants believe that the claims of record now define patentable subject matter over the art of record. Accordingly, an early Notice of Allowance is respectfully requested.

000132722003146411536-1

7